SC402- Introduction to Cryptography
Assignment 4

1. If the factorization of $p-1$ (p prime) is known, then we can verify whether $\alpha \in \mathbb{Z}_p^*$ is a primitive element by making use of the following result.

   Theorem 1. *Suppose that $p > 2$ is prime and $\alpha \in \mathbb{Z}_p^*$. Then α is a primitive element modulo p if and only if $\alpha^{(p-1)/q} \not\equiv 1(\mod p)$ for all primes q such that $q|(p-1)$.*

   Use above Theorem to find the smallest primitive element modulo 97.

2. For $n = pq$, where p and q are distinct odd primes, define

$$\lambda(n) = \frac{(p-1)(q-1)}{\gcd(p-1, q-1)}.$$

   Suppose that we modify the RSA Cryptosystem by requiring that $ab \equiv 1(\mod \lambda(n))$.

   (a) Prove that encryption and decryption are still inverse operations in this modified cryptosystem.

   (b) If $p = 37, q = 79$, and $b = 7$, compute a in this modified cryptosystem, as well as in the original RSA Cryptosystem.

3. Implement the POHLIG -HELLMAN ALGORITHM for finding discrete logarithms in $\mathbb{Z}_p$, where p is prime and α is a primitive element. Use your program to find $\log_5 8563$ in $\mathbb{Z}_{28703}$ and $\log_{10} 12611$ in $\mathbb{Z}_{31153}$.

4. Let $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + x + 28$ defined over $\mathbb{Z}_{71}$.

   (a) Determine the number of points on $\mathcal{E}$.

   (b) Show that $\mathcal{E}$ is not a cyclic group.

   (c) What is the maximum order of an element in $\mathcal{E}$? Find an element having this order.

5. Suppose Alice is using the *ElGamal Signature* Scheme with $p = 31847, \alpha = 5$, and $\beta = 25703$. Compute the values of k and a (without solving an instance of the **Discrete Logarithm** problem), given the signature $(23972, 31396)$ for the message $x = 8990$ and the signature $(23972, 20481)$ for the message $x = 31415$.

6. Suppose we implement the *ElGamal Signature* Scheme with $p = 31847, \alpha = 5$, and $\beta = 26379$. Write a computer program that does the following:

   (a) Verify the signature $(20679, 11082)$ on the message $x = 20543$.

   (b) Determine the private key, a, by solving an instance of the **Discrete Logarithm** problem.

   (c) Then determine the random value k used in signing the message x, without solving an instance of the **Discrete Logarithm** problem.